IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

vs.

BRIAN GARBE,

Defendant.

DEFENDANT'S MOTION TO SUPPRESS AND MEMORANDUM IN SUPPORT

Case No. 19-cr–53

EXHIBIT A

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Wisconsin

In the Matter of the Search of 4512 Coquette Drive, Janesville, WI, including residential building, any outbuildings, and any appurtenances thereto	)	Case No. 18-mj-161 **SEALED**

APPLICATION FOR A SEARCH WARRANT

I, Kevin Wrona, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following premises:

See Attachment A.

located in the Western District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Distribution of child pornography

The application is based on these facts: See attached Affidavit.

☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth in the attached affidavit.

Applicant's signature

SA Kevin Wrona

Printed name and title

Sworn to before me and signed in my presence.

Date: 11-29-18

Judge's signature

Madison, Wisconsin

Magistrate Judge Stephen L. Crocker or
Magistrate Judge Peter A. Oppeneer

AFFADAVIT

STATE OF WISCONSIN)

DANE COUNTY) ss.

I, Kevin C. Wrona, having been duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since 2010, and am currently assigned to HSI Office of the Resident Agent in Charge, Milwaukee, Wisconsin. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, as well as through information provided to me by other law enforcement officers whom I consider to be truthful and reliable. Some of the information was provided in response to administrative subpoenas and search warrants. I believe this information is reliable because it was provided by independent companies in response to court or agency requests.

3. Based upon the information described below, I submit probable cause exists to believe that Brian GARBE used the internet at 4512 Coquette Drive, Janesville, Wisconsin 53546 (subject premises), more particularly described in Attachment A, has committed the crimes of possessing and distributing child pornography, in violation of 18 U.S.C. § 2252 and evidence relating to this crime, more particularly described in Attachment B, can be found at the subject premises.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Anime" refers to refers to Japanese-style cartoon animation that is characterized by colorful graphics, vibrant characters, and fantastical themes, which may or may not include depictions of minors engaged in sexually explicit conduct.

b. "Camera" means a device used for recording visual images in the form of photographs, film, or video signals. Digital cameras record and store images in a digital format, which can include Digital8, MiniDV, DVD, a hard drive, or solid-state flash memory.

c. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone

usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

d. "Child erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. "Child pornography" is defined in 18 U.S.C. § 2256(8), as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. "Cloud" or "cloud storage" is a mechanism in which files can be saved to an off-site storage system maintained by a third party – i.e., files are saved to a remote database instated of the (user's) computer's hard drive. The internet provides the connection between the user's computer and the database for saving and retrieving files.

g. "Computer" is defined pursuant to 18 U.S.C. § 1030€(1) as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices.

h. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

k. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

l. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

m. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

n. A "hash value" is a unique alphanumeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

o. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

p. "Internet Service Providers" ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

q. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment connecting a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter. This MAC address is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

r. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

s. "Records," "documents," and "materials," include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b)

bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

u. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use URLs on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

w. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

x. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

Initiation of Investigation and Overview of "Website M"

6. In March 2012, HSI Phoenix initiated an investigation into a password-protected, fee-based website, identified herein as "Website M,"[1] following an interview with a Website M user ("S1") in connection with a separate child exploitation investigation. S1 allowed HSI agents to assume S1's online identify on Website M, and provided agents with S1's username and password.[2]

7. A user can only locate and access Website M if the user knows its current web address. Once the user enters the correct web address, a box appears that requires the user to enter a "user name" and "password." The user cannot access the site without first entering that information. Once the user enters a valid username and password, Website M's home page appears. The opening page depicts nude anime (i.e., drawings, sketches or cartoons) lasciviously displaying their genitals. The term "Private Club" also appears on the home page

8. Several interviewed Website M members have told agents that they received an e-mail message inviting them to join the site and set up a username and password after they purchased child erotica from another website. Following that purchase, they received a sample image of child pornography along with the question

[1] Law enforcement knows the actual name of Website M. However, the investigation into users of Website M remains ongoing, and public disclosure of Website M's actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or to destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual name and other identifying details of Website M remain undisclosed in this affidavit.

[2] S1 provided SAs with the web address for Website M and S1's login information to Website M but S1 has not provided sufficient information to law enforcement to understand how S1 originally obtained the web address or login information for Website M.

"Are you interested in seeing more of this?" When they clicked "yes," Website M sent them another email with instructions of how to access and join the website.

9. After gaining access to Website M by using S1's user name and login, HSI Phoenix agents determined that it advertises files of child pornography for purchase. Once logged in as a member, the user sees the names of folders available for purchase, which contain previews or samples of images contained in the folders. As of March 2012, the website advertised that it offered 600,000 images and 400 hours of video. Such images and videos are organized into folders, the contents of which can be accessed after downloading them by purchasing a password. At all times relevant to this investigation, Website M hosted its content on a server physically located outside of the United States.

10. Throughout HSI's investigation, Website M has typically charged between $40 USD and $110 USD to purchase the password for encrypted archive files containing multiple images and/or videos of child pornography and child erotica. The majority of archive files cost $89 USD.[3] Once downloaded, the user can "decrypt" the selected archive file by entering in the purchased password to reveal multiple images and/or video files. Phoenix HSI Special Agents have made undercover purchases or accessed several archive files available for purchase, which revealed that most of the archive files

[3] A digital archive file is used to store multiple files within a single, compressed file, which can make it easier to store and transmit numerous files at the same time. File extensions associated with digital archive files include ".rar" and ".zip."

contained between 500 and 2,000 image and/or video files, the majority of which are child pornography.

11. Investigating agents also found that Website M allows members to preview "samples" of the images/videos contained in an archive folder prior to purchase. Investigating agents visited Website M and previewed more than 100 sample folders. Agents found that the majority of the images and videos found in the sample or preview folders depicted apparent minors, and many depicted what appeared to be pre-pubescent minors engaged in sexual activity with adults and/or posed in a sexually explicit manner.

12. Over the course of their investigation, which has involved previewing "samples" and then downloading multiple archive files via Website M, investigating agents have found that the "sample" images and/or video screenshots corresponded to the full sets of image and video files contained in downloaded archive files.

13. After selecting an archive file for purchase, the member pays for its password via credit card. Website M then automatically sends an email to the member with the encryption password for the archive. The member must first download the archive file to a digital device and enter that password to decrypt and de-compress it.

Undercover Purchases Confirmed "Website M" Sells Child Exploitative Material

14. As noted above, HSI obtained membership information to Website M via a consensual takeover of S1's account. Between April 2014 and May 2017, investigating agents made multiple undercover purchases of archive files from Website M.

15. For example, in April 2014, investigating agents (posing as S1) successfully downloaded archive files from Website M. Review of the de-compressed image files, based upon an analysis of hash values, determined that the purchased files included video and image files from a series of images that the National Center for Missing and Exploited Children has identified and verified to depict a pre-pubescent minor child who appears to be less than ten years of age at the time the image was made. Purchased files included the following: "180-2.AVI 9Yo Jenny licked by dog. 16min./with sound." The screenshot for this video depicts a nude, blindfolded, prepubescent female who appears to be less than ten years of age lying on her back while a dog licks her genitals. Over twenty additional pictures from the same series were included, such as an image of the same nude prepubescent female performing fellatio on a dog.

Financial Records Linked to Website M

16. On May 26, 2017, an HSI Phoenix agent, working in an undercover capacity, purchased an archive file from Website M titled "SIBERIAN MOUSE #36." This file was selected because it was listed on the opening page as being newly added (as of January 2017) and agents verified the images within the sample folder contained images depicting apparent minors engaged in sexually explicit conduct. When the investigating agent purchased the "SIBERIAN MOUSE #36" file, the agent received a confirmation email from the email address "TheScript Support" through a payment processor based in the United States that stated, "Your order is currently being processed."

17. HSI agents investigated the link between the U.S. based payment processor and Website M. Investigating agents identified the U.S. company as both a payment processor and online business management tool used by Website M.

18. On July 31, 2017, a federal magistrate in the District of Arizona signed a search warrant for the electronic data in the possession of the U.S. payment processor related to their business transactions with and on behalf of Website M.

19. On August 11, 2017, the U.S. payment processor provided several spreadsheets in compliance with the search warrant. One of the spreadsheets listed all the transactions the company processed on behalf of Website M. This list included over 1,000 purchases made to Website M.

Identifying Brian GARBE as a Purchaser of Child Exploitative Material from Website M

20. In September 2017, HSI analyzed the U.S. payment processor records and identified individuals who made multiple purchases from Website M.

21. The U.S. payment processor records indicate that Brian GARBE made approximately three (3) purchases from Website M between February 2016 and October 2016.

22. According to the U.S. payment processor records, the email address to which it sent the auto-generated receipts and passwords for purchases made by Brian GARBE on Website M was: gtiptop@hotmail.com (the "SUSPECT EMAIL ADDRESS").

23. In response to a summons Pay Pal Holdings, Inc. provided the following subscriber information associated with the Brian GARBE purchaser:

First Name: Brian

Last Name: Garbe

Email: gtiptop@hotmail.com

Address: 4512 Coquette Drive, Janesville, WI 53546

Evidence That Brian GARBE Downloaded Child Exploitive Material from Website M

24. Based upon the U.S. payment processor records, HSI generated the following list of purchases Brian GARBE made via the U.S. payment processor from Website M, along with identifying information linked to each purchase.

Date	File Purchased	First Name	Last Name	Company	Phone	Email	Address
02/27/2016	PHP Script 159	Brian	Brian	Garbe	6083220814	gtiptop@hotmail.com	4512 Coquette Dr., Janesville, WI 53546
03/03/2016	PHP Script 150	Brian	Brian	Garbe	6083220814	gtiptop@hotmail.com	4512 Coquette Dr., Janesville, WI 53546
10/18/2016	Ajax Script 65	Brian	Brian	Garbe	6083220814	gtiptop@hotmail.com	4512 Coquette Dr., Janesville, WI 53546

25. After obtaining Brian GARBE's purchase history from the U.S. payment processor, an HSI Phoenix agent, in an undercover capacity, viewed "samples" from each file named in the above purchase records. The previews were recorded using screen capture software available to law enforcement. In March 2018, through a Letter Rogatory request, HSI obtained an updated image copy of the server used to host Website M. A computer forensic agent verified that the server contained the child

pornography and child exploitative material folders from Website M purchased by Brian GARBE. The forensic agent also located member user names and emails. The forensic agent was able to determine when members logged onto the website, and what IP addresses were used by the member. Brian GARBE was username "topper74," as was found on the server. The username "topper74" signed onto Website M numerous times between September 8, 2015 and March 2, 2018. While records do not indicate GARBE made purchases after October 18, 2016, I believe that each time he signed into Website M, it was to access child pornography, at least through preview windows, which showed samples of the material in each folder. It also demonstrated a continued interest in the child exploitive material on the site.

26. Based on undercover purchases from Website M, investigating agents determined that the only way someone can view the full content of the archive file selected appears to be to: 1) download the archive file from the website and 2) enter the password provided by the website, via email, after payment is verified. There does not appear to be any way to view the full content of folders within the site itself, even with a purchased password.

27. Based on undercover purchases from Website M, the investigation, and my training and experience, it appears that Website M generates a billing name for each archived file available for purchase that corresponds with the name of a commonly purchased "script," in order to disguise the actual contents of the file purchased from the payment processor or anyone else who has access to the billing statement. Note that, in the chart above, all of the purchases contain a title that includes the term

"script." A "script" is computer code or software that makes a computer run smoother and faster. Some examples are "Perl," "JavaScript" and "PHP." It appears Website M named each of the archive files it sells so that it would appear as if its Members purchased "scripts" instead of child pornography. The investigation further revealed that Website M registered its business with the U.S. payment processor under the name "The Scripts" in order to appear as a legitimate company.

28. I viewed the files and folders GARBE purchased. Each archive file contained dozens of images and videos depicting the sexual exploitation of children. The following is an example from each archive file:

(a) File: PHP 159 – File name: "159-2" - this is a video that is six minutes and 42 seconds long, depicting a prepubescent male and prepubescent female performing numerous sex acts upon each other, including masturbation, oral sex and intercourse.

(b) File: PHP Script 150 – File Name: "p1010146a" – this image depicts an adult male penis being pressed against the vagina of a prepubescent female.

(c) File: AJAX Script 65 – File Folder: "Mix" – File Folder: "1" - File Name: "4mo_WILLOW_1" – this image depicts an adult male's erect penis being inserted into the mouth of an infant.

Identification of the GARBE and the SUBJECT PREMISES

29. I reviewed the financial purchase records provided by the U.S. payment processor and noted each of Brian GARBE's purchases listed his billing address as 4512 Coquette Dr., Janesville, WI 53546, the SUBJECT PREMISES.

30. Login records from Website M indicated that user "topper74" logged into Website M nearly exclusively between September 2015 and March 2018, using Internet Protocol address: 71.90.5.213.

31. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 71.90.5.213 was registered to Charter Communications.

32. On or about June 12, 2018, Intelligence Research Specialist Lupe Pruneda issued a U.S. Department of Homeland Security summons to Charter Communications seeking subscriber information concerning the above IP address. The records provided by Charter identified the following account holder as Brian GARBE, with a service address of the Subject Premises. The records also provided a contact e-mail of gtiptop@hotmail.com and cellphone number 608-322-0814, both of which were identified by the U.S. payment processor as having been used to purchase the child exploitative material.

33. A check of publicly available databases also revealed that Brian GARBE resides at the Subject Premises.

34. A check with the Wisconsin Department of Transportation on or about September 25, 2018 revealed that an individual named Brian GARBE, with a date of birth of July 4, 1974, resides at and has a valid Wisconsin driver's license for the Subject Premises.

35. On or about November 9, 2018, representatives of the U.S. Postal Service stated that Brian GARBE is currently receiving mail at the Subject Premises.

36. I conducted surveillance of the SUBJECT PREMISES on or about November 19, 2018 and saw a Chevrolet pickup truck parked on the street in front of it. According to Wisconsin Department of Transportation, this truck was registered to GARBE.

37. On or about November 19, 2018, I used an Apple iPhone wireless device in an effort to gain additional information regarding any potential wireless networks at the Subject Premises. While positioned at the end of the driveway, directly in front of the Subject Premises, I noted there were multiple wireless networks in the area, but all of them were secured. Accordingly, in order to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks as well as my training, experience, and information related to me by agents, I believe that the wireless router at the Subject Premises is likely generating a secured wireless network. As explained above, I know, from my training and experience and information related to me by agents that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

38. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive, possess, and/or access with intent to view child

pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often

maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[4]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography

[4] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Brian GARBE uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A.

39. I believe that GARBE likely displays characteristics common to individuals who possess or access with intent to view child pornography because he is a member of a "members only" website which engages in the distribution of child exploitative material, he has purchased numerous archive files which contained hundreds of images and videos depicting the sexual exploitation of children over a period of several months, and he visited a website dedicated to child pornography numerous times over a two and a half year period.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

40. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which plug into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices.

Individuals can easily store, carry or conceal media storage devices on their persons. Individuals also often carry Smartphones and/or mobile phones.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or

"footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

41. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that forensic examiners can recover computer files or remnants of such files months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how an

individual has used a computer, what the person used it for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that an individual viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

42. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can

record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which the computer created them, although it is possible for a user to later falsify this information.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when someone accessed or used the computer or storage media. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with

user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records sought, a review team cannot always readily review computer evidence or data in order to pass it along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a person used a computer, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because someone used it as

a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain evidence of how Brian GARBE used the computer; sent or received data; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

43. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer

personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures, which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another

seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

44. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password). Wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals

who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

Touch ID

45. I know from my training and experience, as well as from information found in publicly available materials, that some electronic devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") which is read via an integrated biometric device in lieu of a numeric or alphanumeric passcode or password. This feature often referred to as a fingerprint scanner, a fingerprint reader, or for Apple devices, Touch ID.

46. If a user enables the fingerprint scanner on a given device, he or she can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint scanner, which can be found in different locations on the device depending on the manufacturer. In my training and experience, users of devices that offer fingerprint scanners often enable it because it is considered a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

47. In some circumstances, a fingerprint cannot be used to unlock a device that has its fingerprint scanner enabled, and a passcode or password must be used instead. Thus, in the event law enforcement encounters a locked device, the

opportunity to unlock the device via the fingerprint scanner exists only for a short time. The fingerprint scanner also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) too many unsuccessful attempts to unlock the device via the fingerprint scanner are made.

48. If fingerprint scanner enabled devices are found during a search of the premises, the passcode or password that would unlock such devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the fingers of the user(s) of any device(s) found during the search of the premises to the device's fingerprint scanner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the device(s) via fingerprint scanner with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

49. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via the fingerprint scanner, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will

likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the fingerprint scanner of the locked device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via the fingerprint scanner.

CONCLUSION

50. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

Kevin C. Wrona
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 29th day of NOVEMBER 2018.

UNITED STATES MAGISTRATE JUDGE